K A N S A S

JOHN P.SMITH, ADMINISTRATOR

KATHLEEN SEBELIUS, GOVERNOR

DEPARTMENT OF CREDIT UNIONS

DATE: **October 31, 2006**

BULLETIN: **2006-KDCU-CUB-07**

TO: **Management of Kansas chartered credit unions**

SUBJECT: **FFIEC Guidance on Authentication in an Internet Banking Environment**

This Bulletin is to provide notice that in response to FFIEC guidance, KDCU examiners during the next examination will be verifying credit unions have addressed enhanced authentication techniques.

In November 2005, the Federal Financial Institutions Examination Council (FFIEC) and the National Credit Union Administration (NCUA) released changes to privacy and security regulations related to electronic banking (i.e. online banking, telephone banking, etc.) and required mandatory compliance by year end 2006. This guidance was issued under NCUA Letter to Credit Unions 05-CU-18 and most recently 06-CU-13. These references require a completed risk-assessment, enhanced authentication techniques, audit features for monitoring unauthorized activities, and member awareness activities. The following is a brief summary of each. Please note, this summary is not all-inclusive and since each credit union is unique, some institutions may necessitate additional requirements.

Although this guidance addresses risk-based assessments, monitoring/reporting, and member awareness, the primary issues is related to authentication techniques**. Essentially, the FFIEC considers "single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties".** This "single-factor authentication" refers to, for example, only utilizing a user-id and password when logging onto members' online accounts. Due to the recent growth and popularity of transactional websites and more sophisticated methods for account fraud and identity theft, an effective and reliable authentication system must be implemented to safeguard your members' assets.

Risk Assessment

Since each credit union's size, complexity, and strategy are all unique, the standards required for each institutions electronic banking authentication program will similarly be unique. Therefore, enhancement of your authentication methodologies must begin with an electronic banking risk assessment to determine the level of authentication appropriate for your credit union's particular applications.

This risk assessment should:

- ✓ Identify all transactions and levels of access associated with electronic banking customer products and services;
- ✓ Identify and assess the risk mitigation techniques, including authentication methodologies, employed for each transaction type and level of access; and
- ✓ Include the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access.

Although there is no set template for this process, credit unions seeking general information may reference the FFIEC Information Security Booklet (http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm) and the FFIEC IT Examination Handbook, Information Security Booklet (http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm).

Since many credit unions outsource their electronic banking applications, the provider can complete this assessment for the credit union provided you understand it is ultimately the credit union's responsibility for managing risk. The credit union must perform appropriate due diligence when selecting a service provider and can accept the risk assessment performed by the provider after management has determined the assessment is accurate with the solutions provided are sufficient to mitigate risks to the members.

Authentication

The FFIEC has determined that single-factor authentication is inadequate for high risk transactions involving member information or movement of funds to other parties/and/or accounts. Therefore, if your electronic banking applications "permit the movement of funds to other parties and/or the access to customer information...it is 'high risk', necessitating stronger authentication or additional controls", according to the FFIEC.

The following techniques may be used to enhance the credit union's authentication standards:

- ✓ Shared Secrets - Such as customer selected images
- ✓ Smart Cards / Tokens
- ✓ Biometrics - Fingerprint Scanners
- ✓ Internet Protocol Address (IPA) verification
- ✓ Mutual Authentication - Member identity and credit union website is authenticated

Other techniques are listed in the guidance previously referenced. Credit unions should implement an adequate authentication process prior to year end 2006.

Monitoring

A sound authentication system includes audit features that can assist in the detection of fraud, money laundering, compromised passwords, or other unauthorized activities. Although all credit unions should already have transaction monitoring procedures in place to comply with current Bank Secrecy Act regulations, credit unions will need to enhance their procedures to specifically address:

- ✓ Identifying unauthorized transactions
- ✓ Detecting intrusions
- ✓ Reconstructing events
- ✓ Promoting employee and user accountability
- ✓ Identifying suspicious patters

If these services are outsourced to a third party, management must ensure proper logging and monitoring procedures are in place and that suspicious or unauthorized activities are relayed to management in a timely manner.

John P. Smith, Administrator October 31, 2006